

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Missouri

In the Matter of the Search of

INFORMATION ASSOCIATED WITH dfields07964@gmail.com and  
isgriggs.jenni@gmail.com THAT IS STORED AT PREMISES  
CONTROLLED BY GOOGLE LLC.

Case No. 4:23-MJ-6063-PLC

SIGNED AND SUBMITTED TO THE COURT FOR  
FILING BY RELIABLE ELECTRONIC MEANS

## APPLICATION FOR A SEARCH WARRANT

I, Darionte Johnson, a federal law enforcement officer or an attorney for the government,  
request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or  
property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed *(identify the  
person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section - Offense Description*

18 United States Code, Section 1591 (Sex Trafficking of Children by Force, Fraud, or Coercion)

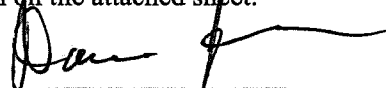
The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested  
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing  
is true and correct.

  
Applicant's signature

Darionte Johnson, Special Agent  
Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedures  
4.1 and 41.

Date: 03/09/2023

Patricia L. Cohen

Judge's signature

City and state: St. Louis, MO

Honorable Patricia L. Cohen, U.S. Magistrate Judge

Printed name and title

AUSA: Dianna R. Collins

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
**dfields07964@gmail.com** and  
**isgriggs.jenni@gmail.com** THAT IS  
STORED AT PREMISES CONTROLLED  
BY GOOGLE LLC.

No. 4:23-MJ-6063-PLC

SIGNED AND SUBMITTED TO THE  
COURT FOR FILING BY RELIABLE  
ELECTRONIC MEANS

**FILED UNDER SEAL**

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Darionte Johnson, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Criminal Procedure 41 for information associated with certain accounts that are stored at premises controlled by GOOGLE LLC, an email provider headquartered at 1600 Amphitheatre Parkway Mountain View, CA 94043 (hereinafter referred to as “the Provider”). The information to be searched is described in the following paragraphs and in Attachment A. The search warrant would require the Provider to disclose to the United States copies of the information (including the content of communications) further described in Attachment B. Upon receipt of the information described in Section I of Attachment B, United States-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a **SPECIAL AGENT** with the FBI and have been since October 2022. Prior to becoming a Special Agent, I was employed with Accenture as a management consultant and Boeing as an analyst, completing supply chain analysis. During my time with the FBI, I worked to support investigations, including violent crimes against children, human trafficking violations, as well as national security investigations.

3. The facts in this affidavit come from my personal observations, my training and experience, as well as information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 United States Code, Section 1591 (Sex Trafficking of Children by Force, Fraud, or Coercion) have been committed by **DONALD EUGENE FIELDS II**, hereinafter "**FIELDS**". Further, there is a reasonable belief that evidence of such crimes are present on accounts owned and/or shared with his paramour, Jennifer Fields (nee Isgriggs), hereinafter "Isgriggs". Probable cause exists to search the location described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

#### **LOCATION TO BE SEARCHED**

5. The locations to be searched are: dfields07964@gmail.com and isgriggs.jenni@gmail.com (hereinafter referred to as "**SUBJECT ACCOUNTS**") located at 1600 Amphitheatre Parkway Mountain View, CA 94043 further described in Attachment A. The items to be reviewed and seized are described in Attachment B.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Eastern District of Missouri: is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).] **AND/OR** [“is acting on a request for foreign assistance pursuant to [18 U.S.C. § 3512].” 18 U.S.C. § 2711(3)(A)(iii).]]

### **BACKGROUND CONCERNING EMAIL**

7. In my training and experience, I have learned that the Provider offers a variety of on-line services, including electronic mail (“email”) access, to the public. The Provider allows subscribers to obtain email accounts at the domain name Gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with the Provider. During the registration process, the Provider asks subscribers to provide basic personal information. Therefore, the computers of the Provider are likely to contain stored electronic communications (including retrieved and unretrieved email for the Provider’s subscribers) and information concerning subscribers and their use of the Provider services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

8. Subscribers can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the Provider. In my training and experience,

evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

9. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

10. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

11. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

12. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or

exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

13. In general, an email that is sent to the Provider is stored in the subscriber's "mailbox" on the Provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the Provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for an extended period of time and, in some circumstances, indefinitely.

14. Therefore, by receiving the requested information from the Provider, additional information about the suspected violation(s) of law and/or the whereabouts of **FIELDS** can be further assessed.

#### **BACKGROUND CONCERNING GOOGLE**

15. I have learned the following about Google:

a. Google offers email services to the public. In particular, Google allows subscribers to maintain email accounts under the domain name Gmail.com. A subscriber using Google's services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Device Information.* Google collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Android ID, Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated



Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

v. *Cookie Data.* Google uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user’s computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

vi. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google’s websites). Google also retains information regarding accounts registered from the same IP address.

vii. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber’s account.

viii. *Preserved and backup records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). Google may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

16. In addition, Google maintains records with respect to other Google Services, which it stores in connection with subscriber accounts, which typically include the following:

a. *Google Drive content.* Google provides users with a certain amount of free “cloud” storage, currently 15 gigabytes, through a service called “Google Drive” (users can purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content “in the cloud,” that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

b. *Google Docs.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called “Google Docs.” Users can use Google Docs to create online documents that can be stored on or saved to the user’s Google Drive.

c. *Google Photos.* Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or “Exif”) data, and can include GPS location information for where a photo or video was taken.

d. *Google Calendar.* Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered

computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

e. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in “chat” sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user’s email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user’s email and chat content.

f. *Location History data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user’s location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device’s most recent location data in connection with a Google account.

g. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

h. *Google Profile.* Google allows individuals to create a Google profile with certain identifying information, including pictures.

i. *Google Plus.* Google hosts an Internet-based social network. Among other things, users can post photos and status updates and group different types of relationships (rather than simply “friends”) into Circles. In addition, Google has a service called PlusOne, in which

Google recommends links and posts that may be of interest to the account, based in part on accounts in the user's Circle having previously clicked "+1" next to the post. PlusOne information therefore provides information about the user of a given account, based on activity by other individuals the user has entered in the user's Circle.

j. *Chrome Browser and Search History.* Google stores information regarding user Internet browser activity when a Google user is logged into his or her account, which includes logging information about websites viewed by the user, Internet search queries in Google Internet search engine available at <http://www.google.com> (and variations thereof, including <http://www.google.ru>), and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

k. *Advertising Data.* Google also stores advertising data, including information regarding unique advertising IDs associated with the customer, devices used to access the account, application IDs, advertising cookies, Unique Device Identifiers (UDIDs), payment information, ads clicked, and ads created.

l. *YouTube Data.* Google owns the video-streaming service YouTube and maintains records relating to YouTube accesses and data posted by the user.

16. Therefore, the computers of Google and are likely to contain stored electronic communications (including retrieved and unretrieved email) for Google subscribers and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

17. As explained above, Google subscribers can also store with the providers files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

18. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

19. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. As explained herein, information stored in connection with a Google account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

**PROBABLE CAUSE**

21. In May 2022, Special Agent Jason Hamlin from the St. Louis Division of the Federal Bureau of Investigation was contacted by Theresa Lustwerk, an officer with the Missouri State Technical Assistance Team (STAT). Officer Lustwerk reported to SA Hamlin that the Franklin County Sheriff's Office began an investigation into **FIELDS** in or about 2017. Officer Lustwerk reported to SA Hamlin that the investigation resulted in an indictment on state charges for statutory rape, statutory sodomy, child molestation and witness tampering in Franklin County Circuit Court in December 2021. A warrant for his arrest was issued by that court after **FIELDS** vacated his home and failed to appear. Your affiant, while not the primary case agent, was involved in a support capacity from approximately June 2022 to present for the case. Your affiant was provided regular briefings about the case from Special Agent Derek G. Velazco and had full access to the case file since that time.

22. After Lustwerk provided this information, Special Agent Hamlin opened an FBI investigation on or about May 2, 2022, into **FIELDS**. The purpose of this investigation was to assist Franklin County Sheriff's Office (FCSO) locate **FIELDS**, a fugitive from the FCSO.

23. During the investigation, SA Hamlin asked Special Agent Derek G. Velazco for assistance with the ongoing investigation due to his experience in investigating sex crimes involving children. At this time, SA Hamlin provided SA Velazco with information about the investigation, to include written and oral briefings about the investigative steps taken until that time. Upon reviewing the case, SA Velazco noted there appeared to be several violations of federal law to include child sex trafficking, as well as the production of child sexual abuse material.

24. As part of the investigation, SA Velazco contacted Officer Lustwerk to discuss the case. Information provided by Officer Lustwerk indicated that as of May 2022 investigators

believed **FIELDS** may be traveling in a 1995 Ford Mustang, purple or maroon in color, license plate NA2 F5V. Additionally, it was reported to SA Velazco that the vehicle was registered to “Ted Sartori.” Ted Sartori was later fully identified as Theodore John Sartori.

25. In October 2022, personnel from the FBI conducted social media analysis of accounts associated with Sartori. A Facebook page ([www.facebook.com/ted.sartori](https://www.facebook.com/ted.sartori), “Ted Sartori”) was located. Posted on or about August 4, 2022, an image of a 1995 Ford Mustang was posted on the account. This material was then reported to Special Agent Velazco and your affiant. The image is included below:



26. Upon further review of the Facebook page, Special Agent Velazco observed a message associated with this image indicated Sartori owned a 1995 Mustang which had recently been painted.



27. On October 6, 2022, Det. Lustwerk provided Special Agent Velazco with a police report from STAT detailing the original allegations against Donald **FIELDS**' sexual abuse of his adopted daughter, K.F.

28. Within this report, it was recorded that K.F. described sexual abuse by both **FIELDS** and Sartori. K.F. reported to Det. Lustwerk she was first raped by **FIELDS** when she was 12 years old. This abuse continued for several years afterwards.

29. In December 2022, both Sartori and **FIELDS** were indicted on one count of Title 18 United States Code, Section 1591, "Sex trafficking of children or by force, fraud, or coercion." On or about December 12, 2022, Sartori was arrested in Girard, MO. **FIELDS** has yet to be located.

30. During the course of the investigation, FBI Staff Operations Specialist Holly Velazco requested postal records for 101 Hambro Ave., Union, MO 63084, an address where **FIELDS** resided prior to his absconding from law enforcement. Results indicated information associated with **FIELDS** and this address were linked to phone number 636-303-7909, with a listed email address of dfields07964@gmail.com. This information was then given to Special Agent Velazco and your affiant.

31. Moreover, on December 14, 2022, Google LLC produced records pursuant to an administrative subpoena for email account dfields07964@gmail.com. This record request returned the following subscriber information:

- a. Name: Jennifer Fields
- b. Created On: 2020-12-31 17:50:07 Z
- c. Terms of Service IP: 24.182.160.118
- d. Last Updated Date: 2022-10-14 22:44:02 Z

- e. Recovery SMS: +16363037909 [US]
- f. IP Activity: No User IP logs
- g. BILLING, TAX, SHIPPING, DEFAULT:

**Don and Jenni Fields**

101 Hambro Ave

Union, MO 63084-1529

+1 636-303-7909

32. These records reflect a connection between dfields07964@gmail.com, an associated PayPal account, and a Yahoo email account. These accounts are registered to **FIELDS** and Isgriggs. During the course of the investigation, Special Agent Velazco was informed by Candy Fields, that Isgriggs was the current paramour and possible wife of **FIELDS**. Candy Fields also reported **FIELDS** and Isgriggs had possibly traveled to Florida and attempted to get married.

33. On December 26, 2022, GOOGLE LLC produced additional records pursuant to an administrative subpoena with a non-disclosure order requesting subscriber records for email account isgriggs.jenni@gmail.com resulting in the following information:

- a. Name: Jenni Fields
- b. Created On: 2015-03-07 03:00:59 Z
- c. Terms of Service IP: 70.195.70.19
- d. Last Updated Date: 2022-01-29 18:29:28 Z
- e. Recovery SMS: 13143655930 [US]
- f. IP Activity: No User IP logs

34. This record return indicated the following individuals are associated with the billing details of the account: **FIELDS** (current husband of Isgriggs), Eric Haegele (ex-husband of Isgriggs), Isgriggs (current wife of **FIELDS**), and Stan Cook (relationship unknown).

35. At this time, **FIELDS** remains a fugitive from justice. However, considering the nature of the investigation, it is assessed that the aforementioned email accounts contain communications that would be helpful in determining Fields current location.

36. Lastly, given the length of time these accounts have been open and the documented owners of record, the Subject Accounts are of significant interest.

37. Records and information such as those identified in Attachment B to the proposed Order will assist the investigative agency (ies) further their investigation by allowing investigators to potentially locate **FIELDS**. At present, investigators do not have any other information which would lead to the speedy locating of **FIELDS**. It is assessed that due to the operational nature of Google's services, it is possible **FIELDS**, or his romantic partner, Isgriggs, may have used the accounts in a manner which would create records assisting in their timely location.

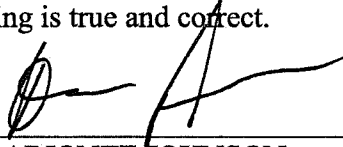
### **CONCLUSION**

38. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on the Provider. Because the warrant will be served on the Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

39. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the

targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.



DARIONTE JOHNSON  
Special Agent  
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 9th day of March 2023.



HONORABLE PATRICIA L. COHEN  
United States Magistrate Judge

**ATTACHMENT A**  
**Property to Be Searched**

This warrant applies to information associated with **dfields07964@gmail.com** and **sgriggs.jenni@gmail.com** that is stored at premises owned, maintained, controlled, or operated by GOOGLE LLC a company headquartered at 1600 Amphitheatre Parkway Mountain View, CA 94043.

**Provider:**  
GOOGLE LLC  
1600 Amphitheatre Parkway Mountain View, CA 94043.

**The Target Account(s):**

The Order applies to certain records and information associated with the following

<b>Facility</b>	<b>Account or identifier</b>	<b>Subscriber, if known</b>	<b>Subject of investigation, if known</b>
GOOGLE LLC	dfields07964@gmail.com Isgriggs.jenni@gmail.com	Donald Eugene Fields II <b>(“FIELDS”)</b> and/or Jennifer Fields (“Isgriggs”)	Donald Eugene Fields II

**ATTACHMENT B**  
**Particular Things to be Seized**

**I. Information to be disclosed by GOOGLE (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The content of all communications sent to or from the account (including through Gmail, Google Hangouts (including videos), and otherwise), stored in draft form in the account, or otherwise associated with the account, including all message content, attachments, and header information.
- b. All address book, contact list, or similar information associated with the account.
- c. Full Google search history and Chrome browser history associated with the account.
- d. All Google Drive content.
- e. All bookmarks maintained by the account.
- f. All services used by the account.
- g. All subscriber and payment information, including full name, e-mail address (including any secondary or recovery email addresses), physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, telephone number, websites, screen names, user identification numbers, security questions and answers, registration IP address, payment history, and other personal identifiers.

- h. All past and current usernames, account passwords, and names associated with the account.
- i. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up.
- j. All YouTube data associated with the account.
- k. All transactional records associated with the account, including any IP logs or other records of session times and durations.
- l. Any information identifying the device or devices used to access the account, including a device serial number, a GUID or Global Unique Identifier, Android ID, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the account;
- m. All activity logs for the account.
- n. All photos and videos uploaded to the account, including in Google Drive and Google Photos.
- o. All information associated with Google Plus, including the names of all Circles and the accounts grouped into them.
- p. All photos and videos uploaded by any user that have that user tagged in them.
- q. All location and maps information.
- r. All Google Voice information.

s. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number).

t. All privacy settings and other account settings, including email addresses or other accounts that the account has blocked.

u. Advertising and Device Data: All advertising data relating to the account, including, but not limited to, advertising cookies, information regarding unique advertising IDs associated with the user, any devices used to access the account, Android IDs, application IDs, UDIDs, payment information (including, but not limited to, full credit card numbers and expiration dates and PayPal accounts), ads clicked, and ads created.

v. Linked Accounts: All accounts linked to the Target Account (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise).

w. For accounts linked by cookie, the date(s) on which they shared a cookie.

x. For accounts linked by SMS number, information regarding whether the numbers were verified; and

y. Customer Correspondence: All records pertaining to communications between the Service Provider and any person regarding the user or the user's account with the Service Provider, including contacts with support services, records of actions taken, and investigative or user complaints concerning the subscriber; and

z. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of the issuance of this warrant.



## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 1591 Sex Trafficking of Children or by Force, Fraud, or Coercion (hereinafter referred to as "the subject offenses"), occurring from October 2011 to present, or relating to **FIELDS** including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence relating to Sex Trafficking of Children by Force, Fraud, or Coercion.
- (b) Evidence relating to communications and connections with foreign governments, entities, and individuals, including evidence relating to the conversion of intellectual property and trade secrets for the economic benefit of a foreign government, foreign instrumentality, or foreign agent.
- (c) information indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime(s) under investigation and to the email account owner.
- (d) Evidence indicating the email account owner's state of mind as it relates to the crime(s) under investigation.
- (e) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any United States personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, analysts, attorney

support staff, and technical experts. Pursuant to this warrant, the investigating agents may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the United States and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF  
DOMESTIC BUSINESS RECORDS PURSUANT TO  
FEDERAL RULE OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by \_\_\_\_\_, and my official title is \_\_\_\_\_.

I am a custodian of records for \_\_\_\_\_. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of \_\_\_\_\_, and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of \_\_\_\_\_; and

c. such records were made by \_\_\_\_\_ as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature